UNITED STATES DISTRICT COURT

for the

District of South Dakota

In the Matter of the Search of:
Electronics Items Identified in Attachment A located in luggage belonging to Marcin Garbacz and currently in the custody of the FBI in Rapid City, South Dakota.

Case No. 5:19-MJ-110

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

SEE "ATTACHMENT A", which is attached to and incorporated in this Application and Affidavit

located in the District of South Dakota, there is now concealed *(identify the person or describe the property to be seized)*:

Evidence of a crime in violation of 18 U.S.C. §§ 2252A and 2251. See Affidavit in Support of Application for Search Warrant, and **ATTACHMENT B**, which is attached to and incorporated in this Application and Affidavit.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 2252A	Possession of Child Pornography
18 U.S.C. § 2251	Production of Child Pornography

The application is based on these facts:

☒ Continued on the attached affidavit, which is incorporated by reference.

☐ Delayed notice of ____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

☐ Your applicant requests that no notice be given prior to the execution of the search warrant, i.e., "no knock", the basis of which is set forth in the attached affidavit.

☒ Your applicant requests authorization to serve the search warrant any time day or night pursuant to Fed. R. Crim. P. 41(e)(2)(A)(ii), the basis of which is set forth in the attached affidavit.

Applicant's signature

Stephen Beery, Special Agent, FBI
Printed name and title

Sworn to before me and:
☑ signed in my presence.
☐ submitted, attested to, and acknowledged by reliable electronic means.

Date: 8-27-19

Judge's signature

City and state: Rapid City, SD

Daneta Wollmann, U.S. Magistrate
Printed name and title

UNITED STATES DISTRICT COURT

for the
District of South Dakota

In the Matter of the Search of

Electronics Items Identified in Attachment A located in luggage belonging to Marcin Garbacz and currently in the custody of the FBI in Rapid City, South Dakota.

Case No. 5:19-mj-110

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the District of South Dakota *(identify the person or describe the property to be searched and give its location)*:

See **ATTACHMENT A**, attached hereto and incorporated by reference

I find that the affidavit, or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized)*:

Evidence of a crime in violation of 18 U.S.C. §§ 2252A and 2251. See Affidavit in Support of Application for Search Warrant, and **ATTACHMENT B**, attached hereto and incorporated by reference.

I find that the affidavit, or any recorded testimony, establishes probable cause to search and seize the person or property.

YOU ARE COMMANDED to execute this warrant on or before Sept 10, 2019 *(not to exceed 14 days)*

☐ in the daytime 6:00 a.m. to 10 p.m. ☒ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to Daneta Wollmann.
(United States Magistrate Judge)

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*

☐ for _____ days *(not to exceed 30)*. ☐ until, the facts justifying, the later specific date of _____.

☐ I find that good cause has been established to authorize the officer executing this warrant to not provide notice prior to the execution of the search warrant, i.e., "no knock".

Date and time issued: 8-27-19 2pm

Judge's signature

City and state: Rapid City, SD

Daneta Wollmann, U.S. Magistrate
Printed name and title

CC: AUSA Patterson & Agent
CLS

Return

Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:
5:19-mj-110		

Inventory made in the presence of :

Inventory of the property taken and name of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

_____
Executing officer's signature

_____
Printed name and title

UNITED STATES DISTRICT COURT
DISTRICT OF SOUTH DAKOTA
WESTERN DIVISION

IN THE MATTER OF THE SEARCH OF: Electronics Items Identified in Attachment A located in luggage belonging to Marcin Garbacz and currently in the custody of the FBI in Rapid City, South Dakota.	CASE NUMBER: 5:19-mj-110 **SEALED** **AFFIDAVIT IN SUPPORT OF SEARCH AND SEIZURE WARRANT APPLICATION**

State of South Dakota)
) ss
County of Pennington)

I, Stephen Beery, Special Agent of the Federal Bureau of Investigation FBI being duly sworn, states as follows:

1. I am an investigative or law enforcement officer of the United States within the meaning of 18 U.S.C. § 2510(7) and am empowered by law to conduct investigation of and to make arrests for offenses enumerated in 18 U.S.C. § 2516. I have been a Special Agent with the FBI since May 2016. As an FBI Agent, I have been assigned to investigate violations of federal law, including the possession, receipt, distribution, and production of child pornography in violation of federal law to include 18 U.S.C. §§ 2252A and 2251. While employed by the FBI, I have participated in numerous investigations in which I have collected evidence in electronic form.
2. I am currently assigned to the Rapid City Resident Agency of the Minneapolis Field Division, which is located in the District of South Dakota. The facts set forth in this affidavit are based on my personal knowledge, information

obtained in this investigation from others, including other law enforcement officers, my review of documents and other records related to this investigation, and information gained through training and experience. Since this affidavit is being submitted for the limited purpose of supporting an application for a search warrant, I have not included each and every fact known to me concerning this investigation, but have set forth only those facts necessary to establish probable cause.

3. Your Affiant is involved in the investigation of a suspected violation of Federal laws by Marcin Stanislaw Garbacz. Your affiant respectfully submits that there is probable cause to believe that Marcin Stanislaw Garbacz committed the crime of possession of child pornography and production of child pornography in violation of 18 U.S.C. §§ 2252A and 2251.

ITEMS TO BE SEARCHED FOR AND SEIZED:

4. Any evidence of the defendant's efforts to entice, harbor, provide, or obtain minors to engage in sexual activity.
5. Any visual depiction of minors engaged in sexual activity, to include but not limited to images and videos.
6. Any written correspondence with minor children or adults describing any sexual acts with minors in any form, including but not limited to emails and text messages.
7. Any other images or video files of criminal activity involving minors.
8. Your affiant respectfully requests that a search warrant be issued to permit a search of the electronic devices identified in Attachment A that were

originally located in luggage belonging to Marcin Stanislaw Garbacz which are currently in the custody of the FBI.

9. I submit that there is probable cause to search for evidence, fruits, and instrumentalities of 18 U.S.C. §§ 2252A and 2251, Possession of Child Pornography and Production of Child Pornography.

DEFINITIONS

10. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. *Chat*: as used herein, refers to any kind of text communication over the Internet that is transmitted in real-time from sender to receiver. Chat messages are generally short in order to enable other participants to respond quickly and in a format that resembles an oral conversation. This feature distinguishes chatting from other text-based online communications such as Internet forums and email.

b. *Child Erotica*: as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not necessarily, in and of themselves, obscene or that do not necessarily depict minors in sexually explicit poses or positions.

c. *Child pornography*: as defined in 18 U.S.C. § 2256(8), is any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually

explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

d. *Cloud-based storage service*: as used herein, refers to a publically accessible, online storage provider that collectors of child pornography can use to store and trade child pornography in larger volumes. Users of such a service can share links and associated passwords to their stored files with other traders of child pornography in order to grant access to their collections. Such services allow individuals to easily access these files through a wide variety of electronic devices such as desktop and laptop computers, mobile phones, and tablets, anywhere and at any time. An individual with the password to file stored on a cloud-based service does not need to be a user of the service to access the file. Access is free and readily available to anyone who has an internet connection.

e. *Computer:* The term "computer" means "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device." *See* 18 U.S.C. §§ 2256(6) and 1030(e)(1). As used herein, a computer includes a cell phone, smart phone, tablet, and other similar devices capable of accessing the Internet.

f. *Computer Hardware:* The term "computer hardware" means all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or

data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices such as video gaming systems, electronic music playing devices, and mobile phones); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, modems, routers, scanners and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

g. *Computer-related documentation*: as used herein, consists of written, recorded, printed, or electronically stored material which explains or illustrates how to configure or use computer hardware, computer software, or other related items.

h. *Computer Passwords and Data Security Devices:* The term "computer passwords and data security devices" means information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates a sort of digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap"

protected data to make it inaccessible or unusable, as well as reverse the progress to restore it.

i. *Computer-Related Documentation:* The term "computer-related documentation" means written, recorded, printed, or electronically stored material which explains or illustrates how to configure or use computer hardware, computer software, or other related items.

j. *Computer Software:* The term "computer software" means digital information which can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

k. *Electronic Communication Service* ("ESP"): as defined in 18 U.S.C. § 2510(15), is a provider of any service that gives to users thereof the ability to send or receive wire or electronic communications. For example, "telephone companies and electronic mail companies" generally act as providers of electronic communication services. *See* S. Rep. No. 99-541 (1986), reprinted in 1986 U.S.C.C.A.N. 3555, 3568.

l. *Electronic Storage Device*: includes but is not limited to external and internal hard drives, thumb drives, flash drives, SD cards, gaming devices with storage capability, storage discs (CDs and DVDs), cameras, cellular phones, smart phones and phones with photo-taking and/or internet access capabilities, and any "cloud" storage by any provider.

m. *File Transfer Protocol* ("FTP"): as used herein, is a standard network protocol used to transfer computer files from one host to another over a computer network, such as the Internet. FTP is built on client-server architecture and uses separate control and data connections between the client and the server.

n. *Internet:* The "Internet" is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

o. *Internet Connection:* The term "Internet connection" means a connection required for access to the Internet. The connection would generally be provided by cable, DSL (Digital Subscriber Line), wireless devices, or satellite systems.

p. *Minor:* The term "minor" means any person under the age of eighteen years. *See* 18 U.S.C. § 2256(1).

q. *Records, documents, and materials*: as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade, photographic, mechanical, electrical, electronic, or magnetic form.

r. *Remote Computing Service* ("RCS"): as defined in 18 U.S.C. § 2711(2), is the provision to the public of computer storage or processing services by means of an electronic communications system.

s. *Short Message Service* ("SMS"): as used herein, is a service used to send text messages to mobile phones. SMS is also often referred to as texting,

sending text messages or text messaging. The service allows for short text messages to be sent from one cell phone to another cell phone or from the Web to another cell phone. The term "computer," as defined in 18 U.S.C. § 1030(e)(1), means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.

t. *Storage Medium:* The term "storage medium" refers to any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

u. *Visual Depictions:* "Visual depictions" include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image. *See* 18 U.S.C. § 2256(5).

v. *Wireless Network:* The term "wireless network" means a system of wireless communications in which signals are sent and received via electromagnetic waves such as radio waves. Each person wanting to connect to a wireless network needs a computer, which has a wireless network card that operates on the same frequency. Many wired networks base the security of the network on physical access control, trusting all the users on the local network. However, if wireless access points are connected to the network, anyone in proximity to the network can connect to it. A wireless access point is equipment that connects to the modem and broadcasts a signal. It is possible for an

unknown user who has a computer with a wireless access card to access an unencrypted wireless network. Once connected to that network, the user can access any resources available on that network to include other computers or shared Internet connections.

PROBABLE CAUSE

11. In December of 2018, Special Agent Brian Pickens, Internal Revenue Service, became aware of an allegation regarding Garbacz's embezzlement of tens of thousands of dollars from the Catholic Diocese of Rapid City (DRC). After becoming aware of these allegations, he opened an investigation.

12. Between December 2018 and May 2019, SA Pickens investigated the allegations, conducted witness interviews, and reviewed Garbacz's financial records.

13. Beginning in July 2012, Garbacz was assigned to various parishes in Rapid City overseen by the DRC. During his residence in Rapid City, Garbacz had access to cash collections at the following parishes: Blessed Sacrament; Cathedral of Our Lady of Perpetual Help; and St. Therese the Little Flower Catholic Church.

14. As part of his compensation for his services to the parishes in Rapid City, Garbacz was paid approximately $22,000 to $24,000 per year. These payments were made to Garbacz utilizing direct deposit into his bank account or by check.

15. Beginning in or about July 2012, and continuing until in or about April, 2018, Garbacz devised and intended to devise a scheme and artifice to

defraud the DRC and enrich himself. As part of the scheme and artifice to defraud, Garbacz would steal and unlawfully divert cash donations made by parishioners at the DRC parishes in Rapid City and deposit them in his own personal bank account at Black Hills Federal Credit Union.

16. Beginning in July 2012, Garbacz began diverting funds from the weekly cash donations for his own personal use. Garbacz would steal and unlawfully divert the cash donations before they were counted and deposited in order to conceal his scheme. In furtherance of his scheme and artifice to defraud, Garbacz would enter the parish at night or in the early morning hours before other parish workers, pastors, or parishioners were there. Garbacz would steal and unlawfully take some cash from the cash donations. Because the amounts were not recorded initially, Garbacz was able to steal the money undetected. After stealing the cash donations, Garbacz would take the cash and deposit it into his personal checking account at Black Hills Federal Credit Union.

17. Based on interviews conducted by SA Pickens of multiple parish workers, SA Pickens learned that there have been concerns about unusually low cash collections at the DRC's Rapid City parishes for a number of years, but parish workers were unable to identify a particular reason. In March 2018, the parish pastor and bookkeeper assigned to the DRC's St. Therese's parish instituted the use of tamper proof cash collection bags and the parish had a video surveillance system installed to try and identify if someone was stealing the cash donations. As a pastor, Garbacz was aware of the decision to begin

using tamper proof bags and knew the access code to the vault room where the cash collections were kept at St. Therese.

18. After the use of tamper proof bags began and after the installation of the surveillance system, Garbacz, in furtherance of the scheme and artifice to defraud, continued to steal and unlawfully divert cash donations. In order to accomplish this, Garbacz purchased his own identical tamper proof bags. Garbacz would then remove the original tamper proof bags from the vault, open them and take a portion of the cash. Once he had removed some of the cash, he would place the remaining cash in his own tamper proof bags and place the new bags in the vault room in order to make it appear that no cash had been stolen. Garbacz would then forge the writing on the new tamper proof bags to make it appear similar to the writing on the original tamper proof bags.

19. After parish workers began using tamper proof bags, they realized the numbers on the bags they reviewed on Monday morning prior to making the deposit were different than the numbers on original bags placed in the vault on Sunday. This fact made the parish workers suspicious that an embezzlement of the cash donations was continuing, but when they reviewed the surveillance footage, they learned it had been turned off or was having technical problems when the suspected thefts of cash occurred and did not record anything.

20. In April 2018, in response to the malfunctioning surveillance system, the bookkeeper at St. Therese's parish installed two additional video surveillance

cameras at St. Therese. Garbacz was unaware these new surveillance cameras had been installed. On Monday, April 23, 2018, at approximately 2:30 a.m. – 3:00 a.m., the surveillance cameras recorded Garbacz removing cash donations from St. Therese and then returning altered bags.

21. On April 23, 2018, Garbacz was confronted by the Bishop for the DRC about the thefts. Garbacz initially denied stealing money, but when confronted with the video evidence, Garbacz admitted to diverting cash donations.

22. In total, between July 2012 and April 2018, Garbacz made cash deposits into his personal bank account in excess of $250,000.00. After being confronted by the Bishop on April 23, 2018, the cash deposits into Garbacz's Black Hills Federal Credit Union Account substantially decreased.

23. On Monday, May 6, 2019, SA Pickens made telephonic contact with Marcin Garbacz in an attempt to conduct an interview. Garbacz chose not to speak about the criminal conduct outlined above. Garbacz was informed that the investigation was ongoing and would continue.

24. After speaking with Garbacz on May 6, 2019, SA Pickens sent a request for a TECS Lookout to be placed on Garbacz to monitor his movement in and out of the United States. On Thursday, May 9, 2019, SA Pickens received confirmation that a TECS Lookout was put in place to identify Garbacz's movements in and out of the United States.

25. On May 10, 2019, SA Pickens was made aware by an agent with the Department of Homeland Security that Garbacz, at 1:05 a.m. on May 10,

2019, scheduled a flight leaving from Seattle-Tacoma International Airport to a final destination of Poland. SA Pickens learned through Homeland Security that Garbacz did not schedule a return flight to the United States. SA Pickens believed Garbacz was attempting to leave the United States as a result of being informed of the ongoing investigation into his criminal conduct and to avoid criminal prosecution.

26. On May 10, 2019, a criminal complaint was filed against Garbacz in the District of South Dakota and an arrest warrant was obtained for Garbacz.

27. On May 10, 2019, special agents with the FBI arrested Garbacz on that warrant at the Seattle-Tacoma International Airport before he boarded his flight. Upon his arrest, the FBI agents seized Garbacz's luggage, which included two large and two medium-sized suitcases, one backpack and one small blue box.

28. After his arrest, Garbacz gave FBI agents permission to obtain his medication from his luggage. Garbacz told agents he did not know which luggage bag his medications were in, just that he knew his medication was in his luggage. Garbacz also told agents he had $10,000.00 in cash in his luggage. Other than obtaining his medication, FBI agents did not search his luggage, but did observe that there were file folders with numerous documents. At least one FBI agent also observed hundred dollar bills in Garbacz's wallet.

29. On May 13, 2019, SA Pickens served a subpoena on and spoke with a representative from JP Morgan Chase bank regarding the current balances

on Garbacz's checking and savings accounts. Between May 8, 2019, and May 10, 2019, just two days after being contacted by SA Pickens and made aware of the investigation, Garbacz withdrew $50,500.00 in cash from his checking and savings accounts, leaving only a few hundred dollars in each. Based on my education, experience, and this investigation, I believe the $50,500.00 is proceeds of Garbacz's illegal activity.

30. On May 16, 2019, a search warrant was obtained to search the luggage seized from Garbacz. FBI agents in Seattle executed the search warrant. During the search, the agents located $10,556 in cash and several religious chalices.

31. During the execution of the search warrant, FBI agents also located the electronic items identified in Attachment A.

32. On July 2, 2019, a search warrant was obtained for the electronic items identified in Attachment A to search for evidence of wire fraud, money laundering, and transportation of stolen property. The search warrant contained a limited scope and your affiant indicated in the affidavit in support of that search warrant that if evidence of a crime not set forth in that affidavit was discovered, a separate warrant would be sought.

33. During the execution of the search warrant, your affiant, using specialized software extracted the files from the electronic items identified in Attachment A. The extractions of the electronic items identified in Attachment A produced several terabytes of data.

34. On August 22, 2019, your affiant was reviewing extracted files and came across what your affiant has reason to believe is child pornography.

35. On the black PNY 32GB thumb drive with grey grip, S/N: 070B667F317FE604, identified in Attachment A, your affiant noted an image and several videos depicting material involving the sexual exploitation of minors. The search of the thumb drive was discontinued immediately pending the issuance of a separate search warrant which would include child exploitation contraband.

36. The file paths and a brief description are as follows:

A. /img_1 B32.EOI/vol_voI5//$CarvedFiles/9829- fll09872.jpg – Image involves a nude male pressing up against another nude male from the back in a sexual manner, while both hold onto a tree in an outdoor setting. The male in front appears to be a minor.

B. /img_IB32.EOl/vol_voI5//$CarvedFiles/11016-fl691696.mov – Video depicts a male from the waist down showering with genitalia visible. The video appears to be taken from under a closed door without the subject's knowledge.

37. Based on the video and data contained within the video and the investigation, your affiant has reason to believe that Marcin Stanislaw Garbacz produced the video file and that the male individual depicted in the video is a minor.

38. Your affiant has reason to believe there may be additional child pornography images and/or videos contained on the electronic items identified in Attachment A. Your affiant's belief is based on the nature of the files contained on the electronic items, including what appears to be image and video files.

Your affiant wishes to draw the Court's attention to the following facts regarding inferences from the above mentioned facts that are based upon my knowledge, training and experience:

39. Through my training and experience I am aware people involved in the online exploitation of children, especially those who are computer-savvy, may use cloud services and may have multiple devices which access the cloud storage device. This may be accomplished utilizing a cell phone, tablet, computer, or other device which has access to the internet.

40. I know that individuals who are involved in the online exploitation of children will often store evidence of their exploitation on their computer system. I also know that when an individual utilizes multiple storage systems, there is often evidence of child exploitation stored in multiple locations.

41. I know that electronic and/or written communication may exist on the computer system, demonstrating the access to an app or website used for the exploitation of minors. I know that exchanging images during chats, such as photos of the offender sent to the minor or vice versa, frequently causes the displayed images to be saved to the hard drive of the computer or in the "images" or "photos" file on a smart phone or tablet. The device may store the images even if the user believes them to be deleted.

42. I know people involved in the online exploitation of children typically associate online with other people with similar deviant sexual interests in children. Accordingly, there is commonly remnants of communications between the offender and other offenders.

43. I know that people who use personal computers and other electronics in their homes tend to retain their personal files and date for extended periods of time; months or even years. Due to a personal computer's unique ability to store large amounts of date for extended periods of time without consuming much additional physical space, people tend to retain this data. Affiant knows this to be true regardless of whether or not a person has traded-in or "upgraded" to a new personal computer. Personal computer users routinely transfer most of their data onto their new computers when making an upgrade. This data transfer is often done by saving files from the old computer to media sources (CD's or floppy disks, etc.) and then saving them to the new hard drive or other external hard drive or storage device. Any evidence of wire fraud, money laundering, or transportation of stolen money is as likely as other data to be transferred to a person's new, replacement or upgraded computer system or to an external storage device.

44. I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted or viewed via the Internet. Electronic files downloaded to a hard drive can be stored for years at little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily-available forensics tools.

45. Based on my training and experience, I know that data can be received by use of a home computer and transferred to other electronic devices, such as

a cell phone. I also know that data or images can be received by use of a cell phone and transferred to a home computer.

46. Based on my own experience and my consultation with other agents who have been involved in computer searches, searching computerized information for evidence or instrumentalities of a crime often requires the seizure of all of a computer system's input and output peripheral devices, related software, documentation, and data security devices (including passwords) so that a qualified computer expert can accurately retrieve the system's data in a laboratory or other controlled environment. There are several reasons that compel this conclusion:

a. The peripheral devices that allow users to enter or retrieve data from the storage devices vary widely in their compatibility with other hardware and software. Many system storage devices require particular input/output devices in order to read the data on the system. It is important that the analyst be able to properly re-configure the system as it now operates in order to accurately retrieve the evidence listed above. In addition, the analyst needs the relevant system software (operating systems, interfaces, and hardware drivers) and any applications software which may have been used to create the data (whether stored on hard drives or on external media), as well as all related instruction manuals or other documentation and data security devices; and

b. In order to fully retrieve data from a computer system, the analyst also needs all magnetic storage devices, as well as the central processing unit (CPU). In cases like the instant one where the evidence consists partly of image files, the monitor and printer are also essential to show the nature and quality of the graphic images which the system could produce. Further, the analyst again needs all the system software (operating systems or interfaces, and hardware drivers) and any applications software which may have been used to create the data (whether stored on hard drives or on external media) for proper data retrieval.

47. Your affiant is aware that conducting a search of a computer system and external hard drives or other electronic storage devices, documenting the search, and making evidentiary and discovery copies for a standard computer can take several business days. Complex systems or recover tasks can require much longer time periods. Due to the back load of computers waiting to be examined and the limited number of trained examiners, any item seized pursuant to this warrant may be examined outside the regular 14-day time period. Further:

a. I know that searching and seizing information from computers often requires investigators to seize most or all electronic storage devices (along with related peripherals) to be searched later by a qualified computer expert in a laboratory or other controlled environment. This is true because of the following: The volume of data stored on many computers and other electronic storage media is typically so large that it is impossible to search for criminal evidence in a reasonable period of time during the execution of the physical search of a search site.

b. Additionally, a suspect may try to conceal criminal evidence; he or she might store it in random order with deceptive file names. This may require searching authorities to examine all the stored data to determine which particular files are evidence or instrumentalities of crime. This sorting process can take weeks or months, depending on the volume of data stored, and it would be impractical and invasive to attempt this kind of data search on-site.

c. In addition, electronic evidence search protocols are exacting scientific procedures designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to inadvertent or intentional modification or destruction, a controlled environment is essential to ensure its complete and accurate analysis.

LIMIT ON SCOPE OF SEARCH

48. I submit that if during the search, agents find evidence of crimes not set forth in this affidavit, another agent or I will seek a separate warrant.

REQUEST TO SEAL

49. I request that the Court order that all papers submitted in support of this application, including this affidavit, the application, the search and seizure warrant, and the Order itself, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is not public. Accordingly, there is good cause to seal these documents because their premature disclosure may jeopardize the investigation.

CONCLUSION

50. Based upon the foregoing, I respectfully submit there is probable cause to believe that the electronic items (identified in Attachment A) contains fruits and evidence of possession of child pornography and production of child pornography. I respectfully request a search warrant be issued for the contents of the electronic (identified in Attachment A)belonging to Garbacz and in the custody of the FBI for evidence of the crime of possession of child

pornography and production of child pornography, in violation of 18 U.S.C. §§ 2252A and 2251.

51. Your affiant states that the electronic items identified in Attachment A are already in the custody of the FBI. Therefore, your affiant asks to be permitted to search the electronic items identified in Attachment A at any time.

Respectfully submitted this 27 day of August, 2019.

Stephen Beery, Special Agent
Federal Bureau of Investigation

Sworn to before me and:
☑ signed in my presence.
☐ submitted, attested to, and acknowledged by reliable electronic means.

this 27th day of August, 2019.

Daneta Wollmann
U.S. Magistrate Judge

Attachment A
Items to be Searched

Electronics Items located in luggage belonging to Marcin Garbacz and currently in the custody of the FBI in Rapid City, South Dakota., and identified as follows:

1. Black iPhone in black case
2. Black Seagate 1TB external hard drive w/ cables S/N: NA7QAV8S
3. Silver and black Seagate 1TB external hard drive w/ cables S/N: NA7JDMA7
4. Black PNY 32GB thumb drive with grey grip, S/N: 070B667F317FE604
5. Orange PNY 4GB thumb drive
6. Black "Case Logic" case with cuff links, adaptor, and nine (9) USB thumb drives
7. Silver Apple laptop model A1706

ATTACHMENT B
Information to be Seized

The following materials, which constitute evidence of the commission of a criminal offense, contraband, the fruits of crime, or property designed or intended for use or which is or has been used as the means of committing a criminal offense, namely a violation of 18 U.S.C. §§ 2252A and 2251, possession of child pornography and production of child pornography:

1. Computers or storage media used as a means to commit the violations described above.
2. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTERS"):
    a. evidence of who used, owned, or controlled the COMPUTERS at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;
    b. evidence of software that would allow others to control the COMPUTERS, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
    c. evidence of the lack of such malicious software;
    d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;
    e. evidence indicating the computer user's state of mind as it relates to the crime under investigation;
    f. evidence of the attachment to the COMPUTERS of other storage devices or similar containers for electronic evidence;
    g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTERS;
    h. evidence of the times the COMPUTERS were used;
    i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTERS;
    j. documentation and manuals that may be necessary to access the COMPUTERS or to conduct forensic examinations of the COMPUTERS;

k. records of or information about Internet Protocol addresses used by the COMPUTERS;
l. records of or information about the COMPUTERS' Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses; and
m. contextual information necessary to understand the evidence described in this attachment.

3. Routers, modems, and network equipment used to connect computers to the Internet.
4. Child pornography and child erotica.
5. Records, information, and items relating to violations of the statutes described above including
   a. Records and information relating to the identity or location of the persons suspected of violating the statutes described above; and
   b. Records and information relating to sexual exploitation of children, including correspondence and communications between Whisper app users.
6. As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).
7. The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones (cell phones), tablets, certain gaming devices, server computers, and network hardware.
8. The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include but are not limited to internal and external hard drives, SD cards, storage disks (CDs and DVDs), flash memory, other magnetic or optical media and "cloud" storage by any provider.